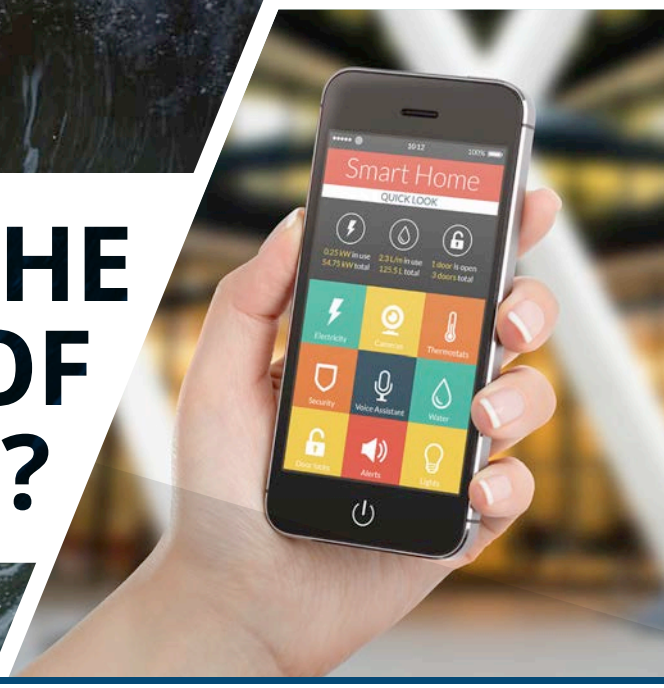
aruba
a Hewlett Packard Enterprise company

HOW TOMORROW MOVES

KEEPING YOUR SANITY AS YOU EMBRACE CLOUD AND MOBILE

There's been lots of buzz about the "tsunamis of change" hitting IT. Talk of pivoting to the cloud, the growing mobile workforce, and the Internet of Things (IoT) light up CIO conferences and generate big headaches for IT. But if you're challenged with growing your business and all these advances can give you an edge, you need to take a closer look. In this period of turbulence, one thing is for sure — to stay competitive, leading businesses will need an integrated networking solution from the access layer to the data center.

This paper aims to change how you think about your enterprise network infrastructure — embracing the opportunities and easing the chaos — so you can design it for the new generation of employees and cloud first, mobile first applications.



WHAT ARE THE TSUNAMIS OF CHANGE?

CLOUD-BASED SERVICES

HR systems, CRM solutions, email, voice and video communications, data storage, point of sale, and many other business services are moving to the private and public cloud. As an IT team, you no longer have to set up these services manually in a server room — you can sign up for them or set them up in your private data center in an afternoon. Instead of taking several weeks, you only have to spend a few days to iron out all the details and start rolling them out to your employees.

MOBILE MADNESS

Mobile devices and apps make it easy for everyone to access cloud-based services. That's the easiest way to explain why the use of smartphones and tablets make sense at work. Cloud-based services are only meaningful when they live on a mobile device. And vice versa — mobile devices are somewhat useless without cloud-based services that are readily available wherever your workforce roams.

THE INTERNET OF THINGS

Back when desktop PCs were cool, one of the most common use cases was to print from the screen onto a piece of paper. These were exciting times and the printer was the IoT device of the day. Fast forward to today and you have many other headless devices that connect to the wired or Wi-Fi network: Apple TVs, Chromecast adapters, security sensors, and video cameras among others.

Instead of a desktop PC, the mobile device is the remote control that interacts with this new class of IoT devices and we manage these IoT devices in the cloud. Without an open mind to embrace cloud-based services and enable the pervasive use of mobile at work, investment in IoT is doomed to fail.

MOBILE-CLOUD IS THE NEW SERVER-CLIENT

It's clear that the mobile-cloud model is replacing the server-client model of yesterday. This model comes with considerable time savings and increased simplicity in how a business app is deployed and accessed. It's not very surprising then to see all the buzz about these changes in IT circles.

While the cloud first/mobile first model sounds good on paper, it has significant implications on how you design your network infrastructure. In fact, these two tsunamis will most definitely cause chaos in how you manage and secure your network.

NETWORK CHAOS: THE CHALLENGES FACING IT

SECURITY AND ACCESS CONTROL

As you embrace this new normal, the notion of separate campus, branch and remote network access disappears. If an employee shows up with an iPad, connects to the network and accesses the cloud-based business service, that location is an extension of your mobility infrastructure. This entire end-to-end mobility infrastructure needs to have the same security and quality of service policies defined for cloud apps and mobile devices — there can be no exceptions. In the past, we didn't care about how we deployed and managed Ethernet ports across different locations, since none of us carried our desktop PCs in our backpack.

From a security standpoint, things get trickier when you consider that mobile devices move outside of buildings. Employees connect to hotspot networks in coffee shops or to the 4G LTE network where you lose control completely. What happens to that device while out in the wild is a mystery, one that causes nightmares if you don't have an easy way to deal with an infected mobile device connecting back to the enterprise network.

GOODBYE ETHERNET PORT, HELLO MOBILE CONTEXT

From a networking perspective, the identity of a user is no longer an Ethernet port number. The new mobile context — role of the user in an organization, the type of mobile device they're using, the types of apps running on that device, and where the device is located — are all useful context points to define policies before we allow network access.

An end user can be a guest, employee, contractor with employees from different departments — all connecting to the same Wi-Fi radio. Each device can be personally owned or corporate-issued. Each device may not run the same operating system, and none of the owners will ask permission to download a new mobile app from the app store. Who knows if they're even installing the latest updates. From an IT standpoint, this is sheer chaos!

DEFINE YOUR NETWORK USERS

With the new normal, every new networking project depends on requirements for mobility, and every mobility infrastructure depends on the needs of #GenMobile — tech-savvy users who demand anytime, anywhere connectivity. We strongly recommend identifying who your network users are before starting with the network design. For example, in a school district, administrators who need mobile UC tools as they roam between different schools have different needs compared to students who need to access online exams in the classroom. In healthcare, family and friends of patients need good Internet connectivity to stay connected with their loved ones in common areas, while doctors and nurses need to access confidential electronic health records on an iPad as they visit patients in each room. In these and many other examples, the expectation is that the same network serves them all.

CAN YOU CLEARLY IDENTIFY WHO — STUDENTS, DOCTORS, EXECUTIVES — WILL CONNECT TO YOUR NETWORK, AND WHAT BUSINESS APPS THEY'LL USE?

EASING THE PAIN WITH SOFTWARE-DEFINED NETWORKING

DO YOU HAVE THE RIGHT SET OF TECHNOLOGY IN YOUR NETWORK TO EASE THE PAIN?

You may call it Software-Defined Networking (SDN) or programmable networking, but what do these tech terms really mean? They make your life simple as you try to organize the chaos in your network.

CONNECT HUNDREDS OF BRANCH LOCATIONS

Assume that you deploy IoT devices at your branch offices and you want to secure every single Ethernet port that they connect to, with traffic inspection and analysis. It makes sense since today's IoT devices are commercial grade and they use proprietary non-standards based protocols that are higher risk. With a SDN controller in your data center, it is possible to push intelligence to hundreds of access switches at these locations with the touch of a button. Keeping your wired ports safe at the branch does not have to mean weeks of manual switch provisioning or software upgrades. The days of manually configuring access points and switches are long gone. Now you can install remote access points in your employee's home and switches at your branch locations without any manual provisioning done onsite, thanks to cloud-based provisioning of these units.

GET READY FOR WI-FI CALLING

Your existing wireless LAN will start to serve a new type of traffic very soon — Wi-Fi calling. This technology enables phone calls on your smartphone to use Wi-Fi instead of the cellular network, as long as you have good connectivity. With a mobility controller in your data center, you should be able to program thousands of access points with the push of a new configuration, and automatically have them identify and prioritize Wi-Fi calling.

DEPLOY MOBILE BUSINESS APPS IN A SNAP

Today's workforce depends on new and exciting business applications. Skype for Business, formerly known as Microsoft Lync, is clearly one of them. Chat, voice, video, screen share and file transfer are all available within one small app icon. It seamlessly integrates with your contact list inside Microsoft Exchange, allowing you to find your colleagues by typing their name on your touchscreen — say goodbye to 4-digit extensions. With Skype, all traffic is encrypted and there is almost no way to identify the type of traffic flow the app is generating unless you can directly integrate with the Skype server using its SDN API. It is practically impossible to configure every single switch and access point to talk directly to the server, so SDN and mobility controllers come to the rescue. Once they identify the type of traffic on your network, they instruct their siblings as to which applications to prioritize, for who, and on which device.

PROTECT YOUR NETWORK FROM THE ONSLAUGHT OF THREATS

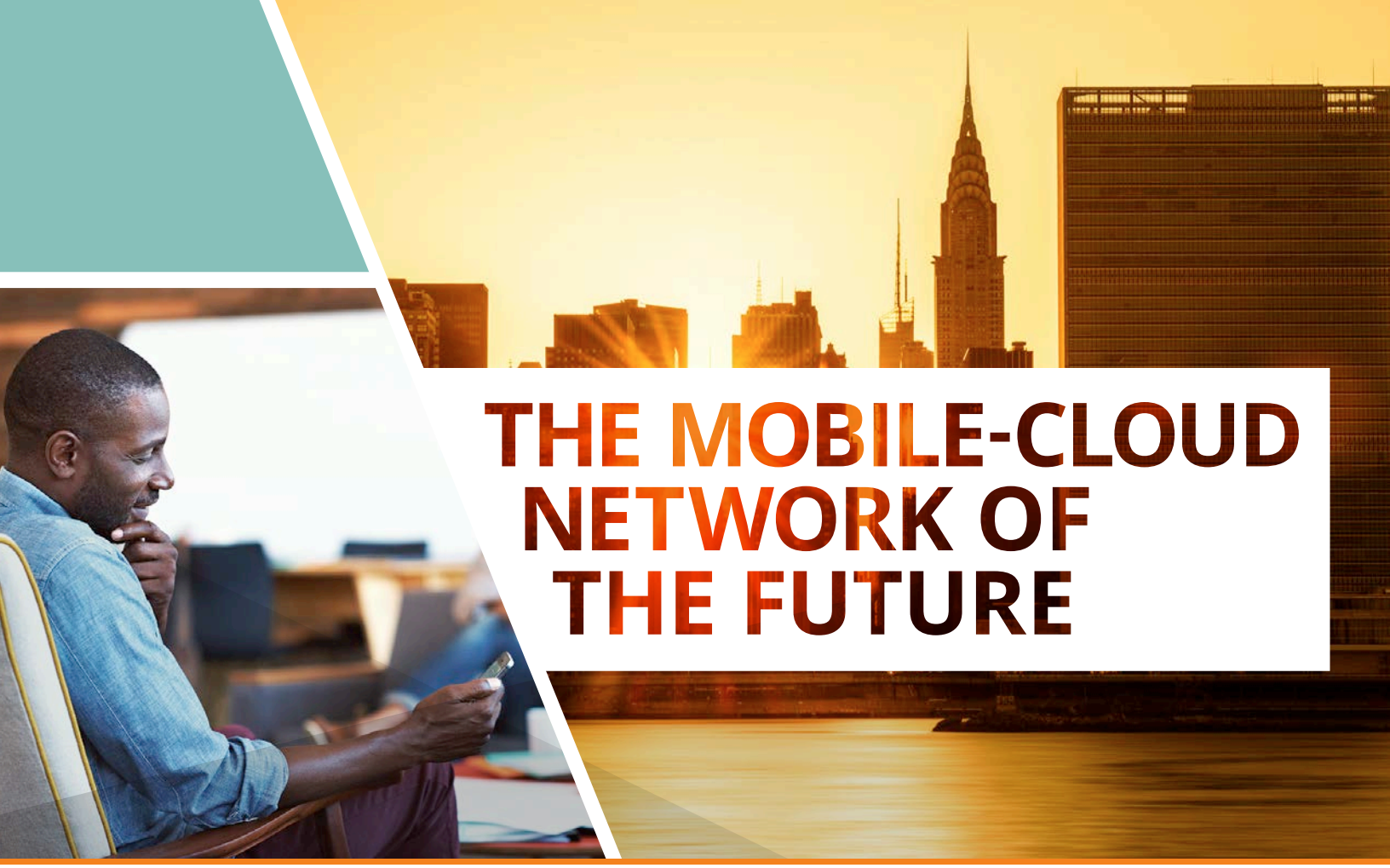
Your next generation network access control solution should make everything else in your network smarter about IoT and mobile devices. If a mobile device is infected with malware and your WAN firewall is intelligent enough to detect it, should that mobile device still be assigned the same network access rights? Absolutely not! Your network should adapt.

Your access control solution should inform the Wi-Fi infrastructure about the state of this device, and place it in a quarantine role until the security risk is eliminated. To help with the process, your access control solution can notify the end user through mobile notifications of what just happened, and what the next steps are to guide them through the process of "self-healing." The fact that you will not have to deal with keeping thousands of mobile devices healthy and that you can offload the responsibility to the end users, and to the programmable network infrastructure, should come as a breath of fresh air. Talk about saving time and operational dollars.

DYNAMICALLY INTERCONNECT THINGS OVER YOUR NETWORK

The Internet of Things can deliver smart spaces — intelligent meeting areas, location services, and real time monitoring are just a few applications that can make the workplace more efficient and productive. The possibilities are endless — but in the new IoT world, sensors and devices often work poorly on enterprise networks and can't protect themselves. With the right set of network software controls, things like Apple TV and Google Chromecast work securely and as intended.

As an example, imagine if a coworker asked you to enable screen sharing for a guest's Android smartphone on a Google Chromecast device in your meeting room. Now imagine being on the guest network and trying to get access to an IoT device that's under IT control. While this once seemed impossible, it can now be done with the right network software controls.



THE MOBILE-CLOUD NETWORK OF THE FUTURE

The shift to mobile-cloud has changed how we think about enterprise networking. It has also been the driving force behind Hewlett Packard Enterprise and Aruba joining forces. This combined company can now offer an integrated solution that spans the access layer to the data center. We serve businesses that want to stay ahead of the game, support their mobile workforce anywhere, and deploy business apps at warp-speed.

Businesses are no longer shackled to an outdated networking model defined by client server computing. Using software programmability that extends across the network, you can adapt in real time to the demands of #GenMobile. This new network understands contextual information such as where the user is, what applications they're using, and which devices are connecting. It can also assign and enforce policies based on a complete view of the end point (in the case of IoT) or the user. The combined HPE-Aruba approach stands in stark contrast to the legacy networking designs that continue to rely on over-engineered hardware platforms and a methodology that focuses on adding more Ethernet ports, rather than enhancing the user experience through software. With HPE and Aruba, your business can move towards the new digital workplace with speed, security, and simplicity at the forefront.

aruba
a Hewlett Packard Enterprise company

Ready to take the next step?

Contact Sales